03-07-00 A

jc781 U.S. PTO 03/06/00

PATENT APPLICATION TRANSMITTAL LETTER
(Small Entity)

Docket No. 1424-8124

TO THE ASSISTANT COMMISSIONER FOR PATENTS

jc678 U.S. PTO 09/519187 03/06/00

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:

William H. Zinger and Jerry A. Krill

For: **SOFTWARE PROTECTION FOR SINGLE AND MULTIPLE MICROPROCESSOR SYSTEMS**

Enclosed are:

- ☒ Certificate of Mailing with Express Mail Mailing Label No. **EG124451055US**
- ☒ **5** sheets of drawings, 9 pages specification, 3 pages claims, 1 page Abstract
- ☐ A certified copy of a application.
- ☒ Declaration ☒ Signed. ☐ Unsigned.
- ☒ Power of Attorney
- ☐ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☒ Verified Statement(s) to Establish Small Entity Status Under 37 C.F.R. 1.9 and 1.27.
- ☐ Other:

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	9	- 20 =	0	x	$0.00
Indep. Claims	8	- 3 =	5	x $39.00	$195.00
Multiple Dependent Claims (check if applicable) ☐					$0.00
				BASIC FEE	$345.00
				TOTAL FILING FEE	$540.00

- ☐ A check in the amount of to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **01-2218** as described below. A duplicate copy of this sheet is enclosed.
  - ☐ Charge the amount of as filing fee.
  - ☐ Credit any overpayment.
  - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
  - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: 3/6/00

Signature

Carla Magda Krivak
Registration No. 30,956
Office of Patent Counsel
The Johns Hopkins University
Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

JHU/APL Docket No. 1424-8124

In re application of: Zinger et al.

For: Software Protection for Single and Multiple Microprocessor Systems

Box Patent Application
Assistant Commissioner for Patents
Washington, D. C. 20231

EXPRESS MAIL CERTIFICATE

"Express Mail" label number EG124451055US

Date of Deposit: 3/6/00

I hereby certify that the following attached patent application as identified above consisting of the following:

1. Postcard receipt
2. Patent Application Transmittal Letter (1 page) (in duplicate)
3. Verified Statement Claiming Small Entity (3 pages)
4. Declaration and Power of Attorney for Patent Application (3 pages)
5. Specification (9 pages); claims (3 pages); 1 Abstract and 5 sheets of drawings

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to Box Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Christina F. Carr

Christina F. Carr

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) AND 1.27 (d)) - NONPROFIT ORGANIZATION	Docket No. 1424-8124

Serial No.	Filing Date	Patent No.	Issue Date

Applicant/ Patentee: **William H. Zinger and Jerry A. Krill**

Invention: **SOFTWARE PROTECTION FOR SINGLE AND MULTIPLE MICROPROCESSOR SYSTEMS**

I hereby declare that I am an official empowered to act on behalf of the nonprofit organization identified below:

NAME OF ORGANIZATION: **THE JOHNS HOPKINS UNIVERSITY**

ADDRESS OF ORGANIZATION: **34th and Charles Streets**
Baltimore, MD 21218

TYPE OF NONPROFIT ORGANIZATION:

- ☒ University or other Institute of Higher Education
- ☐ Tax Exempt under Internal Revenue Service Code (26 U.S.C. 501(a) and 501(c)(3))
- ☐ Nonprofit Scientific or Educational under Statute of State of The United States of America
  Name of State: Citation of Statute:
- ☐ Would Qualify as Tax Exempt under Internal Revenue Service Code (26 U.S.C. 501(a) and 501(c)(3)) if Located in The United States of America
- ☐ Would Qualify as Nonprofit Scientific or Educational under Statute of State of The United States of America if Located in The United States of America
  Name of State: Citation of Statute:

I hereby declare that the above-identified nonprofit organization qualifies as a nonprofit organization as defined in 37 C.F.R. 1.9(e) for purposes of paying reduced fees to the United States Patent and Trademark Office regarding the invention described in:

- ☒ the specification to be filed herewith.
- ☐ the application identified above.
- ☐ the patent identified above.

I hereby declare that rights under contract or law have been conveyed to and remain with the nonprofit organization with regard to the above identified invention.

If the rights held by the above-identified nonprofit organization are not exclusive, each individual, concern or organization having rights to the invention is listed on the next page and no rights to the invention are held by any person, other than the inventor, who could not qualify as an independent inventor under 37 CFR 1.9(c) or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

☒ no such person, concern or organization exists.
☐ each such person, concern or organization is listed below.

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: **Carla Magda Krivak, Esq.**

TITLE IN ORGANIZATION: **Office of Patent Counsel, Applied Physics Laboratory**

ADDRESS OF PERSON SIGNING: **11100 Johns Hopkins Road**
Laurel, MD 20723-6099

SIGNATURE: _____ DATE: 3/6/10

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

On this 5th day of March, 1997, as Vice Provost for Research of The Johns Hopkins University, I hereby authorize Francis A. Cooch and Carla Magda Krivak, patent attorneys at The Johns Hopkins University/Applied Physics Laboratory, to act on behalf of The Johns Hopkins University in matters relating to the execution of Verified Statements Claiming Small Entity Status filed with the U.S. Patent and Trademark Office pursuant to 37 CFR 1.27.

Theodore O. Poehler
Vice Provost for Research
The Johns Hopkins University

STATE OF MARYLAND

CITY OF BALTIMORE

On this 5th day of March, 1997, before me personally appeared Theodore O. Poehler, Vice Provost for Research of The Johns Hopkins University, a corporation of the state of Maryland, and executed the foregoing instrument for the purposes therein stated.

In witness whereof I hereonto set my hand and official seal.

Mary Angela Gornowsky
(NOTARY)

(SEAL)

My Commission Expires May 1, 2000

1424-8124

SOFTWARE PROTECTION FOR SINGLE AND MULTIPLE MICROPROCESSOR SYSTEMS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of prior filed co-pending U.S. Provisional application No. 60/122,984, filed on March 5, 1999.

STATEMENT OF GOVERNMENTAL INTEREST

This invention was made with Government support under Contract No. N00024-98-D-8124 awarded by the Department of the Navy. The Government has certain rights in this invention.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention provides both software and data protection for single or multiple microprocessor systems such as, local area networks (LANs), wide area networks (WANs), backplane connected processor architecture, etc. More particularly, the present invention provides protection by employing, singly or in combination, obscurant IC coatings, tamper detection and response circuitry, multiple component modules and software code encryption to prevent software from being stolen or altered. Similarly, encryption can be applied to data bases and streaming data to provide protection.

Description of the Related Art

Commercial processor boards contain several components with a central processing unit (CPU) as a separate component from volatile and non-volatile memory. Often, the executable code for sets of applications is stored in some device, possibly removable, such as but not limited to, a floppy disk, hard drive, CDROM, or EPROM. The executable code is easily accessible to unauthorized parties and, if not encrypted, can be easily reconstructed in any of a number of formats that would facilitate unauthorized modification or use. Even when supplied in encrypted form, the need to decrypt the code before sending it to the processor makes it available on accessible connections where it

can be collected by appropriate probes in its decrypted form. Thus, even use of key encryption, whether public/private key or some other type, does not stop the pirating, sabotaging or accessing of computer programs that may be proprietary. A parallel argument applies to databases and on-line streamed data. Coating of multi-chip components, for example, multiple custom IC chips on a common substrate, has been proposed to protect knowledge of custom circuitry logic and inter-chip interaction, for example. Although using the emerging technology of commercial coatings on individual integrated circuit chips or components can protect the decrypted program from being read directly by obscuration from electrical or radiative probing, it does not prevent access to probing inter-component conductor paths over which data and code are transferred. This information can easily be read by probing between components.

Thus, nothing has been done to protect computer programs and data passing between components in processors, whether custom or general-purpose commercial processors such as those used in personal computers and workstations.

SUMMARY OF THE INVENTION

It is an object of the present invention to prevent software, databases and streamed data in processors from being stolen, sabotaged or accessed.

It is a further object of the present invention to protect the software or database not only during transport but also during downloading into a processor or processor network and during execution and storage of the code or database within the host system.

It is another object of the present invention to provide protection with no slow-down in processing system performance when it is used to protect software and databases.

It is yet another object of the present invention to use obscurant coatings and tamper detection and response circuitry, singly or in combination, multiple component modules and software code and data encryption in a manner to protect software and data passing between components.

It is yet another object of the present invention to provide a non-standard processor circuit board with respect to its architecture and component arrangement as compared to related art.

It is a further object of the present invention to provide a processor circuit board capable of interacting in standard fashion with other standard processor boards and components over back-plane busses, LANs, WANs and other interconnection methods.

These objects are achieved by providing a novel form of a general-purpose processor/computer having at least three integrated circuit (IC) components mounted on a single substrate as a multi-component module (MCM) including a CPU, one or more memory chips and one or more custom chips containing at least one each of a de-encryption key and algorithm for converting an encrypted computer program as it is received over a bus from a non-volatile memory. Further, an obscurant coating can be used to cover the chips, interconnection circuits and other elements within the multi-component module. The obscurant coating can be used alone or in combination with tamper detection and response circuitry, or the tamper detection and response circuitry may be used alone. The multi-component chip module can be provided in a bus configuration with other multi-component chip modules and one or more memory chips.

Alternatively, the de-encryption may be built into the CPU chip, or a computer program operating in the CPU could perform the de-encryption.

A method for protecting a processor system from tampering is also provided by mounting IC components on a single substrate as a multi-component chip module, converting an encrypted computer program, encrypted code or encrypted data into its original unencrypted form, sending the de-encrypted computer program, code or data to appropriate locations in memory located in the multi-component chip module, protecting these memory locations from external access, and protecting the multi-component chip module using one or a combination of obscurant, deceptive patterns and tamper detection/destruction mechanisms.

These objects, together with other objects and advantages which will be subsequently apparent, reside in the details of construction and operation as more fully described and claimed hereinafter, reference being had to the accompanying drawings forming a part hereof, wherein like reference numerals refer to like parts throughout.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a prior art processor board in a back-plane buss environment;

Figure 2 is a block diagram of the architecture of the tamper resistant computer system according to the present invention;

Figure 3 is a block diagram of a processor board having an encryption processor located thereon according to the present invention in a back-plane buss environment;

Figure 4 is a block diagram of a processor board having multiple encryption processors located thereon according to the present invention providing for encryption processes applied separately to code and data with feed-through of un-encrypted code and data in a back-plane buss environment; and

Figure 5 is a block diagram of a processor board having direct, in-line, real time de-encryption and encryption logic in a back-plane buss environment.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is directed to a tamper resistant processor system that prevents software, databases or streamed data from being stolen due to piracy, sabotage i.e., virus or unauthorized modification, or access to proprietary algorithms and/or stored/processed data, in addition to other vulnerabilities. The present invention protects the software, database or streamed data during transport and also during downloading into a processor or processor network. In addition, it also protects the software, database or streamed data during execution and storage of code within the host system.

Normally, commercial processor boards contain several components. As shown in prior art Figure 1, a central processing unit (CPU) is a separate component from volatile and non-volatile memory components, which store executable code as well as input data and processed data. Code or data is, for example, supplied from a card that is external to the processor board. This code or data could be supplied on the card in encrypted form so that the code or data would be protected if the card were to be obtained by an unauthorized person. The encryption technique can include public/private key encryption, etc. However, the lines of code or data must be decrypted prior to execution or other authorized use. It is at this point where the re-translated code or data is stored

and accessed by a processor/controller that a skilled tamperer could access the code or data for unauthorized use. For example, probing the connections between components allows decrypted code or data transfers from memory to the CPU to be accessed and reconstructed. Commercial coatings are beginning to appear for use on individual integrated circuit chips or components to protect the decrypted program from being directly read by way of obscuration from electrical or radiative probing. Tamper detection and response chips are being developed that can take appropriate action, say clearing memory, when a tamper attempt is sensed. Encryption/decryption processes are being considered for incorporation in computer chip sets to prevent unauthorized access from network connections. However, these techniques do not prevent access to probing inter-component conductor paths over which data and code are transferred.

The present invention overcomes this problem and prevents access to probing inter-component conductor paths by using the known approaches of obscurant IC coatings, tamper detection and response circuitry, multiple component modules and software code encryption in a novel way to protect software when computing, and particularly, in general purpose computing.

For example, an obscurant coating is placed on chips, interconnection circuits and other elements within a module housing, so that if a laser or optical device tries to detect information, the information cannot be read. Further, the adhesive nature of the obscurant, coupled with module lid construction, can prevent its removal without irretrievably damaging the IC and the information contained thereon. Tamper detection and response circuitry could clear memory, destroy the de-encryption key and alter the de-encryption circuitry, for example.

The present invention will first be described for the case in which only a computer program code is to be protected.

As shown in Figure 2, lines of code in a computer program (or programs) are first encrypted **(1)** so that each line is coded with a protected random encryption sequence. This generally requires an encryption algorithm with a unique encryption key to randomly "seed" the algorithm. Thus, the same key and corresponding algorithm are the only direct way to decode the program lines of code. This is a conventional cryptography practice. It is important that the "crypto key" and algorithm be protected at the encryption

site by standard security measures. The encrypted code is entered into a nonvolatile memory **(2)** such as a soft or hard disk or, as shown in Figure 2, an erasable, programmable read only memory (EEPROM) component mounted on a flash memory PC card, etc. This allows the program to be readily transported and stored, yet be protected by its encrypted form. This is another known approach.

To access and use this program in a manner that is protected from tampering, the present invention has been proposed. The present invention includes a general-purpose processor/computer (processor board). The processor board of the present invention differs from prior art devices in its architecture and component arrangement.

One example of an architecture and component arrangement of the processor board according to the present invention is shown in Figure 3 where code alone is being protected. As shown in Figure 3, three or more IC components are mounted on a single substrate as a multi-component module (MCM) **20**. The components of this processor board include a CPU **22**, which can be a standard commercial CPU, and memory chips including volatile memory **23** (DRAM or equivalent) and non-volatile memory **26** (Flash memory, EEPROM, etc.). In addition, a new type of custom chip **24** contains a de-encryption key input and algorithm. Memory controller **25** operates to select between secured memory and unsecured memory. Thus, an additional unsecured memory **27** can not access internal memory. Further, processor buss **28** functions within the MCM **20** via the memory controller **25** so that unencrypted data from, for example, the additional unsecured memory **27** is isolated from encrypted data, etc.

Figure 2 illustrates how the encrypted code and the de-encryption key are brought together at the computer system. Under CPU **22** and memory controller **25** control, the key is loaded from a flash memory **26** within the MCM **20**. The chip **24** then converts, for example, in this case, the encrypted computer program as it is received over, for example, a bus **28** from the Flash memory **26**, into its original unencrypted form and, under CPU **22** control, sends the de-encrypted program(s) to appropriate locations in memory IC(s) **23, 26**, etc., that are located in the MCM **20**. Thus, the complete computer program to be executed is available to the processor from high-speed memory in unencrypted form. This arrangement removes de-encryption delays to the start-up process allowing the CPU **22** direct access to the critical instruction access path of the

processor during program execution, thereby providing code protection, yet full processing system performance.

In an alternative architecture, the de-encryption circuit could be made a part of the CPU **22** chip, thereby reducing the chip count in the MCM **20**. In yet another example, a computer program operating in the CPU **22** could perform the de-encryption. When processing speed does not need to be maintained, this software approach could run continuously, reducing the memory requirements within the MCM **20**. The current art would allow incorporation of sufficient high-speed memory within the MCM **20** to contain very large computer programs. The components within the MCM **20** housing, including the custom chip **24** (crypto-processor chip), CPU **22** and memory ICs **23, 26**, etc., mounted on a common substrate, can be coated with obscurants, provided with unused and deceptive patterns, and/or provided with tamper detection/destruction mechanisms. These will serve to protect the de-encryption key and algorithm, the stored de-encrypted computer program(s) and the intermediate processed data that is temporarily stored in the module memory that could reveal processing algorithms of the protected computer programs. The resulting processor board can be commercially produced and yet retain the same connector pin locations, voltages and software support as current commercial boards. It should be noted that although the above has been described with regard to an encrypted computer program, the present invention is also applicable to encrypted code and encrypted data.

Figure 4 shows the addition of data path encryption/de-encryption to the code protection circuitry in Figure 3. Here the capability to maintain processor performance without affect from the encryption/de-encryption circuit would be dependent on the size of the data memory within the MCM **20** compared to the data base size, or to the timing nature of the streamed data.

Figure 5 shows a configuration using a direct, in-line, real time de-encrypt logic chip **40**. In this configuration, the delay through the de-encrypt logic chip **40** adds to memory access time. For data protection, the MCM **20** would encrypt output to the memory.

With respect to employing obscurants on the MCM **20**, types of obscurants that can be used include, for example, BORDEAUX, Chipseal™ (Dow Corning), etc., but are

not limited thereto. BORDEAUX offers, for example, an economical wafer level protective technology which includes screen printing of an opaque layer followed by the deposition of an etch resistant material to inhibit the reverse engineering of an integrated circuit. The coating provides protection using a thin layer on the integrated circuit of approximately 10-25 μm. The obscurant coating is compatible with plastic, ceramic and multichip assemblies and is inexpensive.

Thus, the present invention provides a new processor board, commercial or otherwise. An encrypted computer program is stored in the non-volatile memory **26** such as an EEPROM, Flash memory, etc.. The non-volatile memory board **26** can be operated itself or as part of a bussed or local area network (LAN) architecture with connectivity to processor boards. The more general multiple processor network will be considered first in describing the invention. Upon powering up the computing network, the various computer programs stored in the non-volatile memory **26** are sent to their addressed destinations on each of the processor boards. This is a standard process. Next, according to the novel features of the present invention, on the special processor boards, as shown in Figs. 2 and 3, appropriate programs are routed into the de-encryption component **24** within the destination processor's multi-chip module **20**. Then, after each program line of code has been decrypted using the key and algorithm stored at appropriate locations in the multi-chip module **20**, the code is sent from the de-encryption component to the appropriate memory locations in the memory components also located in the MCM **20**. Each of the processors is now ready to perform its processing functions by their respective CPUs using their memory on the module, as does a conventional processor, with no performance affect due to the code de-encryption process. Further, input/output data are sent through the same input/output interfaces as a conventional board. That is, it goes from/to other processors for further operations, or to a system input/output. Or, as embodied in Figure 4, input/output data itself may be de-encrypted/encrypted with, possibly, some small reduction in total processing performance.

The present invention can be used on specialized or personal computer configurations. In a personal computer, the configuration would vary from Fig. 2 in that the Flash Memory PC Card **26**, shown would be replaced with a floppy, CDROM or hard disk/drive, for example, for insertion of the encrypted computer program(s). Thus, there

would be only one of the above-described processor boards of the above-described design. In addition, the bus **28** could be replaced with a direct interface to the disk drive. The process for program down loading, de-encryption and operation would be the same as described above.

Thus, the general processor board of the present invention, in a bus configuration with other boards or as a single board and a non-volatile memory such as an EEPROM, Flash memory, etc., protects the software, encryption process, and intermediate data from compromise. It should be noted that this configuration would allow the board to be interchanged with a conventional board one-for-one in an existing system, subject to implementation of the encryption process. Further, the present invention can protect entire local area networks (LANs), wide area networks (WANs), backplane connected processor architecture, etc., such that all the computer programs, software and data on the network, etc., is protected. Subject to the use of an adequately secure encryption technology, this approach would permit system operation of LANs and WANs at multiple levels of classification. Need- to- know and classification level would be controlled by the key assigned to individuals. This key could be an alphanumeric sequence used in a conventional password entry format, or it could be a physical device similar to the key used to enable and set security level for secure telephone systems. The data would remain in its encrypted form everywhere in the network except at key controlled input and output devices. The network could then handle a range of security levels and content access permissions. It should be noted that the present invention is not limited to the examples mentioned above.

The foregoing is considered as illustrative only of the principles of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and applications shown and described, and accordingly, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention and the appended claims and their equivalents.

IN THE CLAIMS:

1. A tamper resistant processor system, comprising:

a multi-component chip module (MCM) including:

a CPU;

one or more memory chips; and

one or more chip means containing at least one each of a de-encryption key and algorithm therein; and

an obscurant covering the contents of said multi-component chip module.

2. A tamper resistant processor system according to claim 1, further comprising said multi-component chip module in a bus configuration with other multi-component chip modules and said one or more memory chips.

3. A tamper resistant processor system, comprising:

processor boards;

an encrypted computer program;

a non-volatile memory, operatively connected to said processor boards, for storing said encrypted computer program and sending said encrypted computer programs to address destinations on said processor boards;

multi-component chip modules for receiving and de-encrypting said encrypted computer program and sending said de-encrypted computer programs to memory components on said multi-component chip modules.

4. A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate as a multi-component module or as the contents of a multi-component module;

b) converting an encrypted computer program, received over a bus from a non-volatile memory, into its original un-encrypted form;

c) sending the de-encrypted computer program to appropriate locations in memory located in the multi-component module; and

d) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanisms.

5. A tamper resistant processor system, comprising:

processor boards;

encrypted code;

a non-volatile memory, operatively connected to said processor boards, for storing said encrypted code and sending said encrypted code to address destinations on said processor boards; and

multi-component chip modules for receiving and de-encrypting said encrypted code and sending said de-encrypted code to memory components on said multi-chip modules.

6. A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate a s a multi-component module or as the contents of a multi-component module;

b) converting encrypted code, received over a bus from a non-volatile memory, into its original un-encrypted form;

c) sending the de-encrypted code to appropriate locations in memory located in the multi-component module; and

d) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanism.

7. A tamper resistant processor system, comprising:

processor boards;

encrypted data;

a non-volatile memory or network data source, operatively connected to said processor boards, for storing said encrypted data and sending said encrypted data to

address destinations on said processor boards and for receiving and storing encrypted data resulting from the processing of the input data; and

multi-component chip modules for receiving and de-encrypting said encrypted data, sending said de-encrypted data to memory components on said multi-chip modules, for storing the results of processing the de-encrypted data, and for encrypting the results before sending to storage or network external to the multi-component chip modules.

8. A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate as a multi-component module or as the contents of a multi-component module;

b) converting encrypted data, received over a bus from a non-volatile memory, into its original unencrypted form;

c) sending the de-encrypted data to appropriate locations in memory located in the multi-component module;

d) encrypting processing result data that is being sent to storage or networks external to the multi-component module; and

e) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanisms.

9. A tamper resistant processor system, comprising:

a multi-component chip module including:

a CPU; and

an in-line real time de-encryption chip;

one or more memory chips, operatively connected to said in-line real time de-encryption chip, said multi-component chip module encrypting out put to said one or more memory chips; and

a memory controller selecting between secured and un-secured memory over a processor buss.

ABSTRACT

Protection is provided for software and data in single and multiple microprocessor systems, including, but not limited to, local area networks (LANs), wide area networks (WANs), backplane connected architectures, etc. The data can include databases, streaming data and code. The protection is provided by employing, singly or in combination, obscurant IC coatings, tamper detection and response circuitry, multiple component modules and software code encryption to prevent software from being stolen or altered. The software or data is protected during transport, during downloading into a processor or processor network, and also during execution and storage of code or a database within a host system. The data product resulting from processing within the protecting equipment may be encrypted to be sent safely to external locations were it may be stored or de-encrypted for further use.

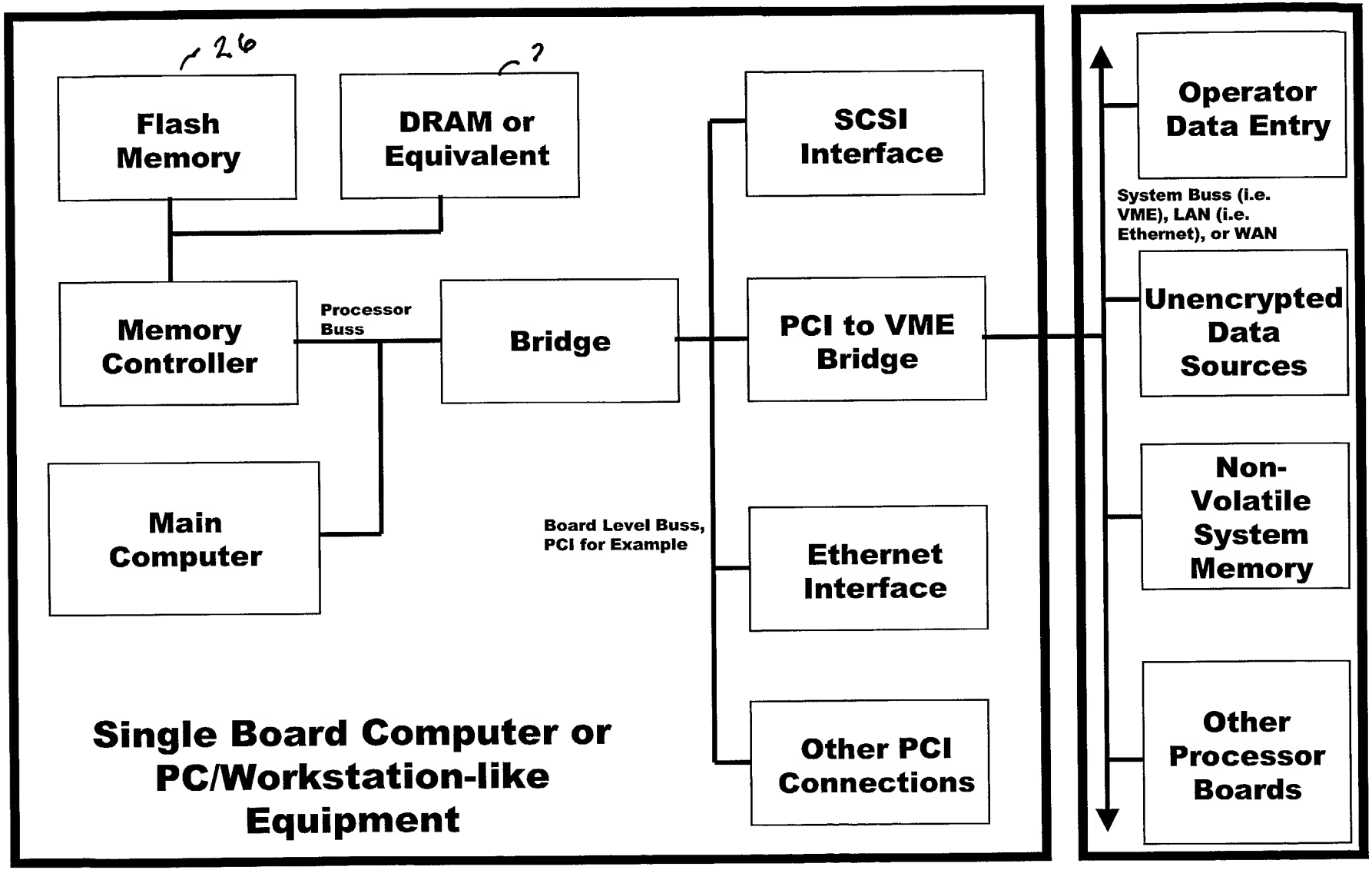

Fig. 1 Prior Art Processor Board Connected to Typical System Elements

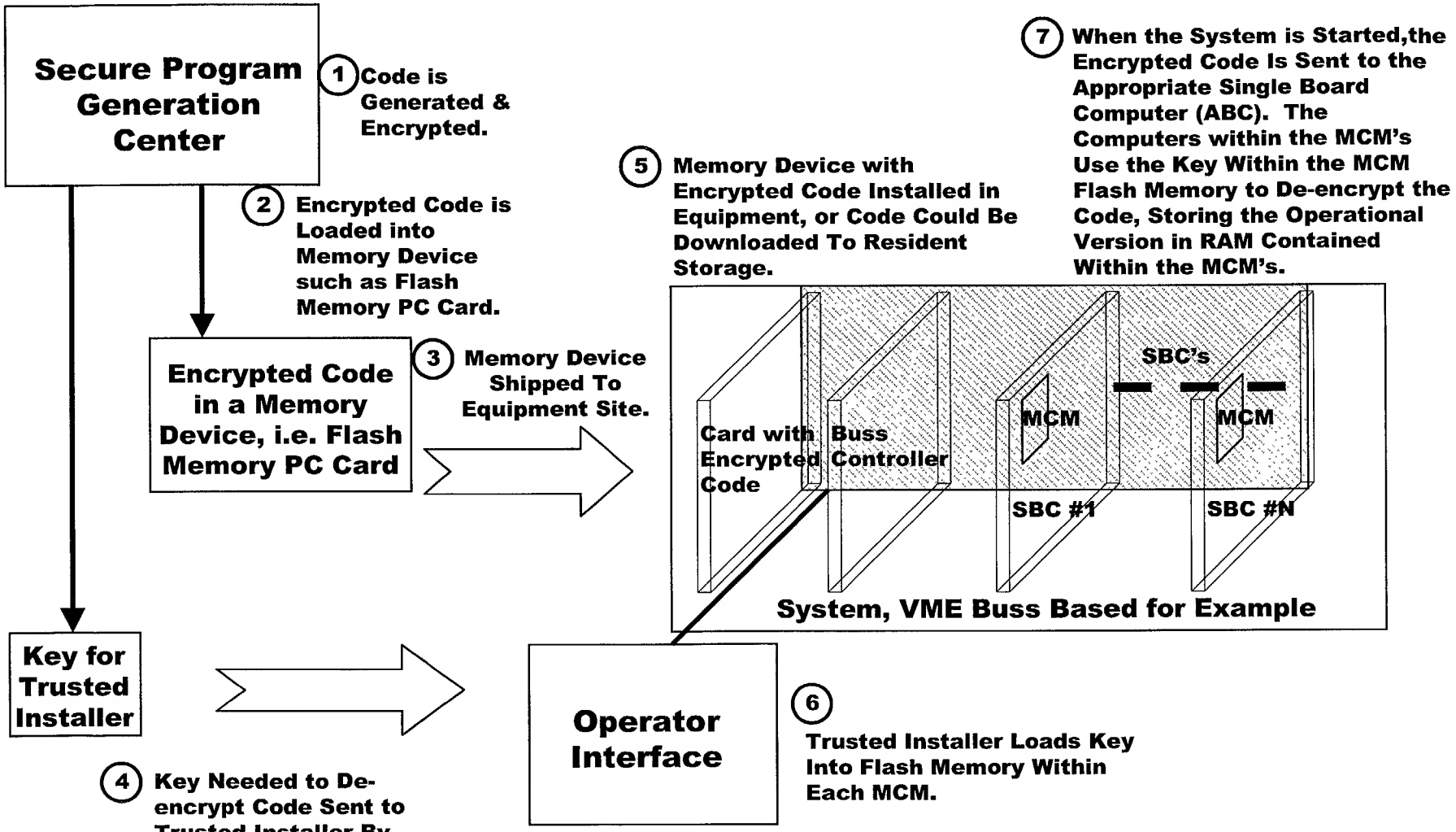

Fig. 2 Architecture For A Tamperproof Computer System

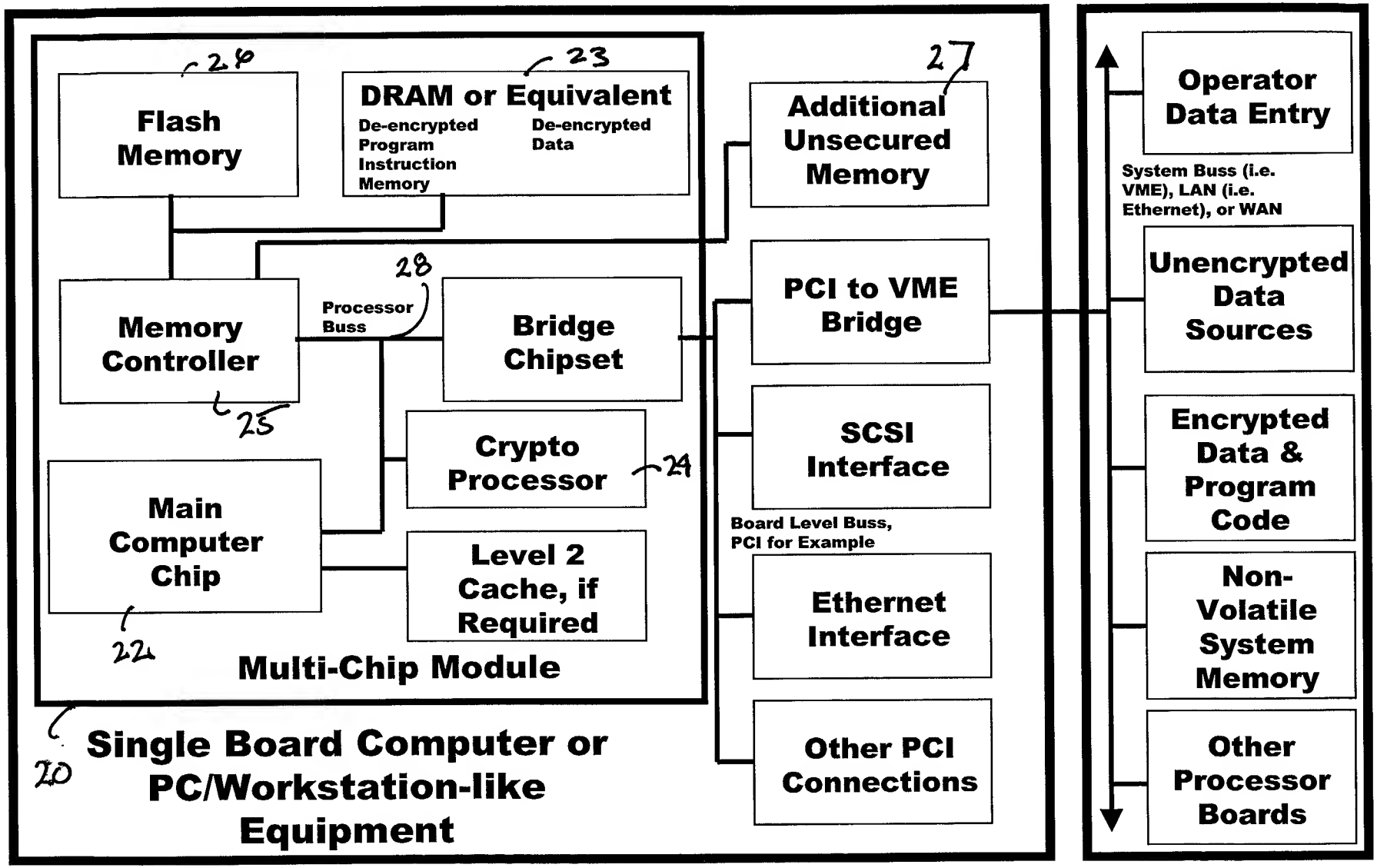

Fig. 3 Processor Board With De-Encryption Within A Multi-Chip Module

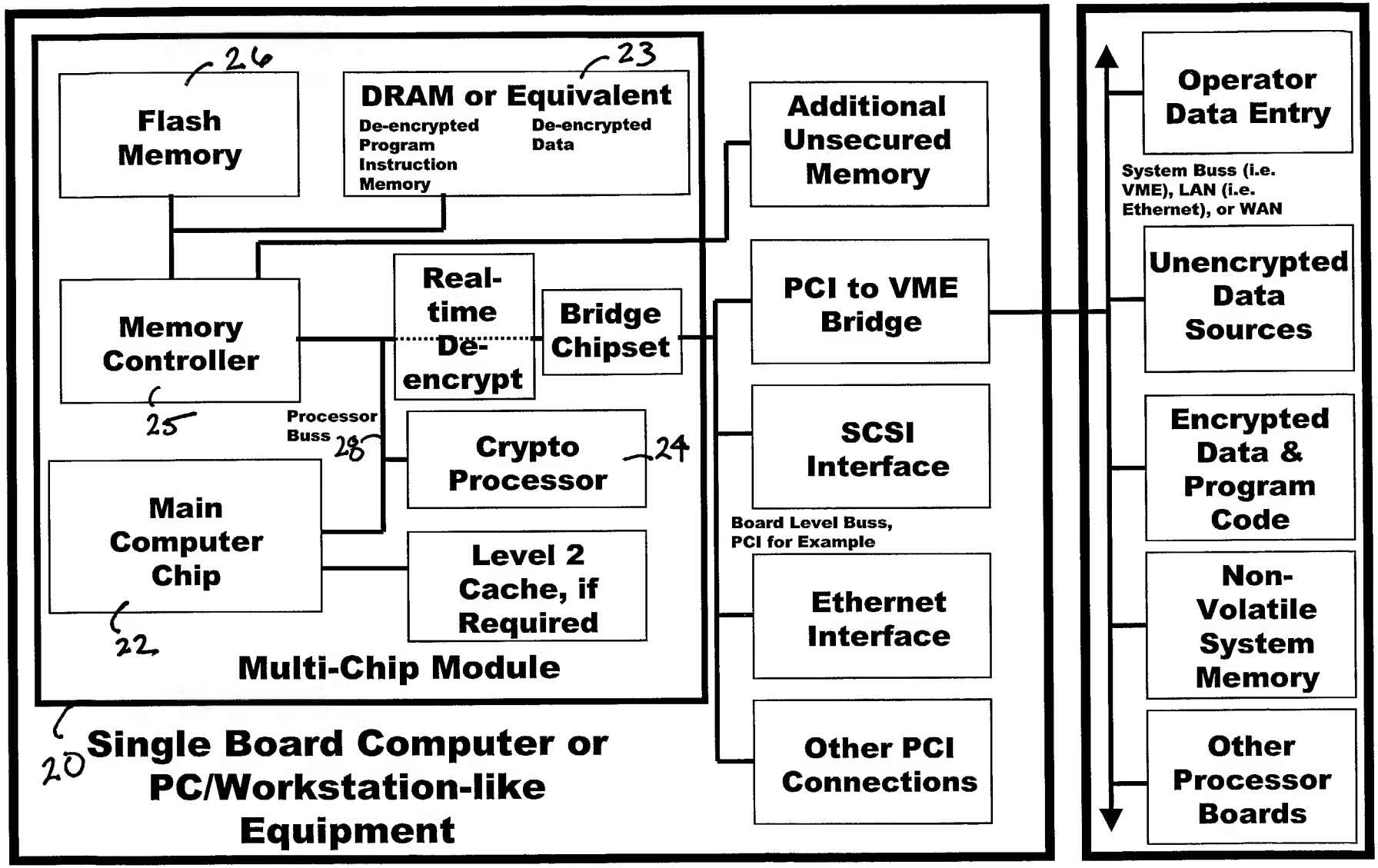

Fig. 4 Processor Board With Multiple De-Encryption Devices Within A Multi-Chip Module

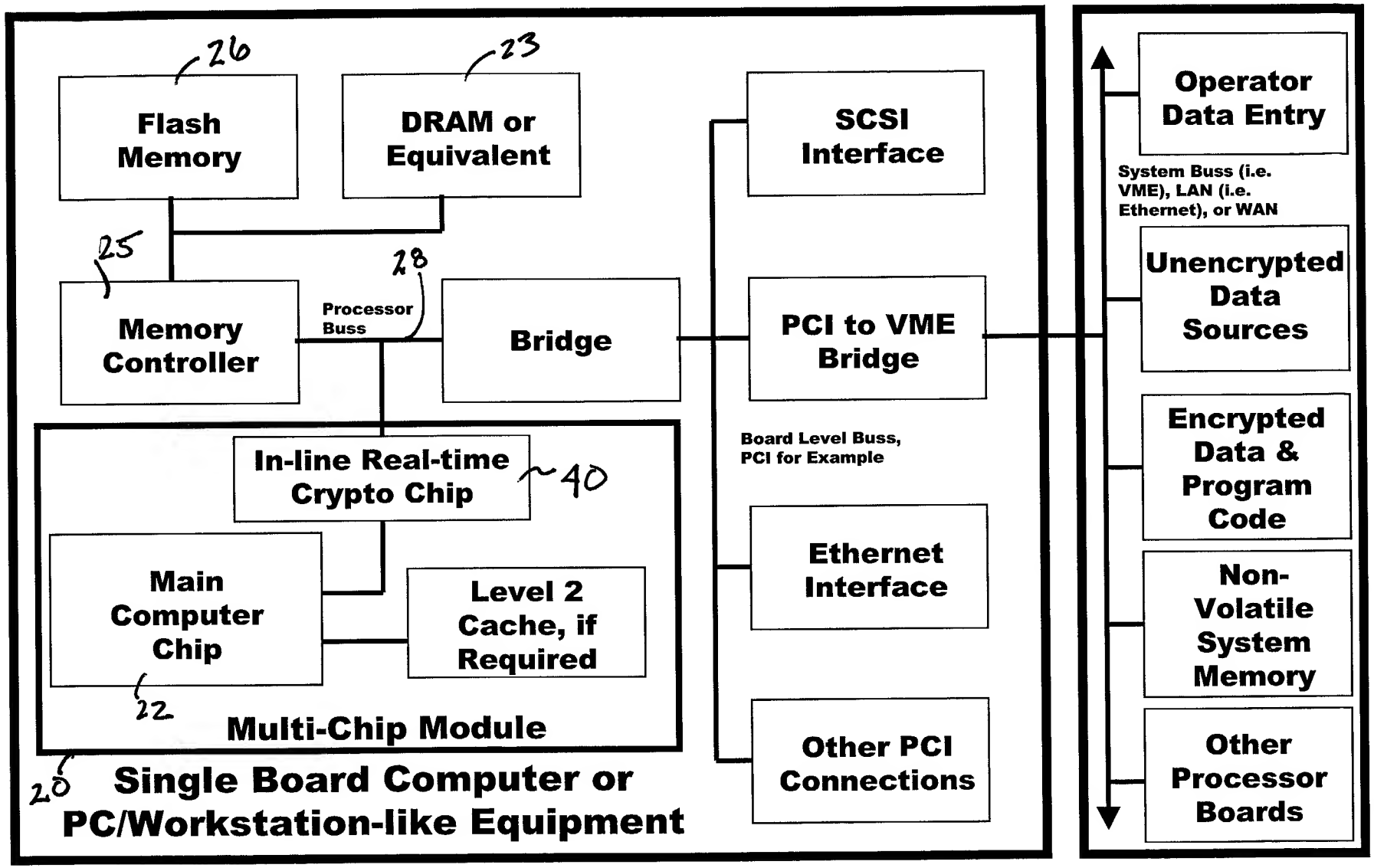

Fig. 5 Processor Board With In-line Real-time De-Encryption Within A Multi-Chip Module

Docket No.
1424-8124

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SOFTWARE PROTECTION FOR SINGLE AND MULTIPLE MICROPROCESSOR SYSTEMS

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International Application Number _____

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

60/122,984	March 5, 1999
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Carla Magda Krivak, Registration No. 30,956 **Francis A. Cooch, Registration No. 31,495**

☐ Send Correspondence to: **Carla Magda Krivak, Office of Patent Counsel**
The Johns Hopkins University/Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099

Direct Telephone Calls to: *(name and telephone number)*
Carla Magda Krivak (240) 228-5644

Full name of sole or first inventor
William H. Zinger

Sole or first inventor's signature — Date: 3/3/00

Residence
10344 Maypole Way, Columbia, Maryland 21044

Citizenship
U.S.A.

Post Office Address
10344 Maypole Way, Columbia, Maryland 21044

Full name of second inventor, if any
Jerry A. Krill

Second inventor's signature — Date: 3/3/00

Residence
4057 Firefly Way, Ellicott City, Maryland 21043/2

Citizenship
U.S.A.

Post Office Address
4057 Firefly Way, Ellicott City, Maryland 21043/2